

**User based authentication on FSSO, using LDAP and FSSO agent on advanced mode.**

Applicable Firmware version: v5.0 and v5.2

### Requirements:

User based authentication required on FSSO, so different users get different profiles through policy. Need to integrate FortiGate with LDAP, install FSSO agent (with DC Agent) on the server with advanced mode and set user filter from FortiGate FSSO configuration using LDAP.

### Integrate FortiGate with LDAP:

The screenshot displays the 'Edit LDAP Server' configuration window in the FortiGate GUI. The left sidebar shows the navigation tree with 'User & Device' selected. The main area contains the following fields and options:

- Name: ldap
- Server IP/Name: 192.168.1.222
- Server Port: 389
- Common Name Identifier: sAMAccountName
- Distinguished Name: dc=chandru,dc=local
- Fetch DN: (button)
- Bind Type: ☐ Simple ☐ Anonymous ☒ Regular
- User DN: administrator@chandru.local
- Password: (masked with dots)
- Secure Connection: ☐
- Test: (button)
- OK: (button)
- Cancel: (button)

config user ldap

edit "ldap"

set server "192.168.1.222"

set cnid "sAMAccountName"

set dn "dc=chandru,dc=local"

set type regular

set username "administrator@chandru.local"

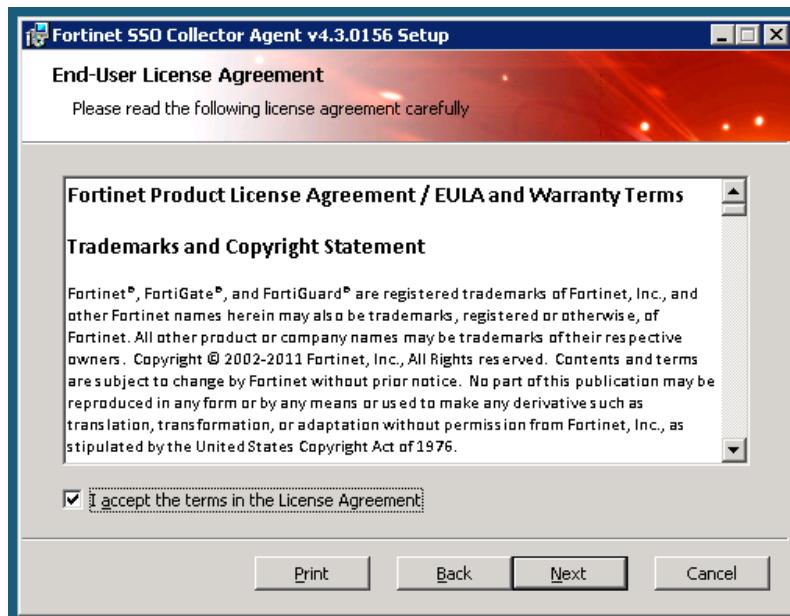
set password XYZ

next

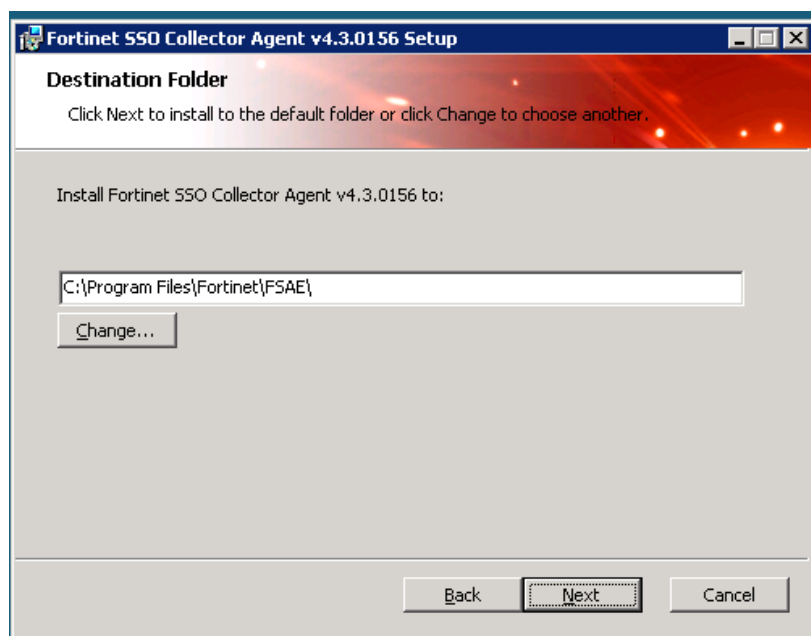
end

Install FSSO agent on the Server on Advanced mode:

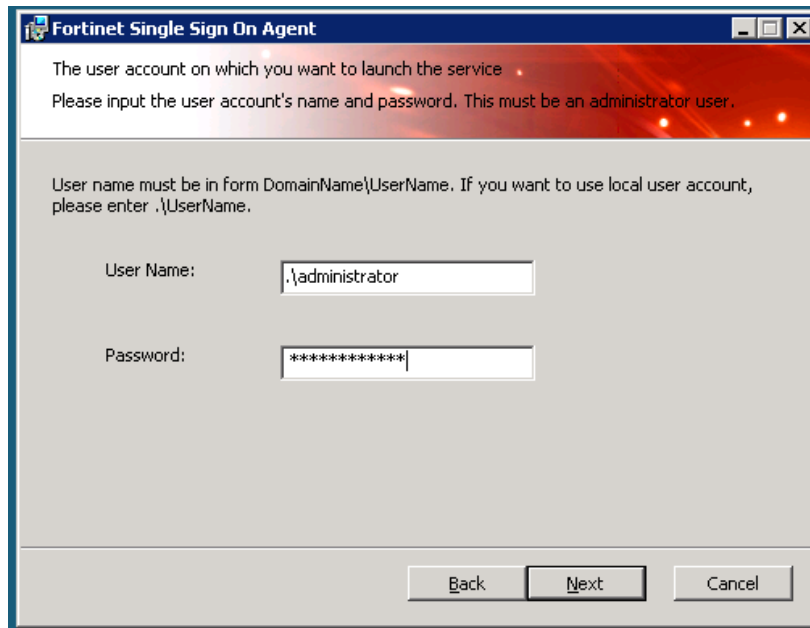
1) Accept the agreement.



2) Change the location if you require, however make sure you have the default location :



### 3) Enter the domain admin credentials



The user account on which you want to launch the service .  
Please input the user account's name and password. This must be an administrator user .

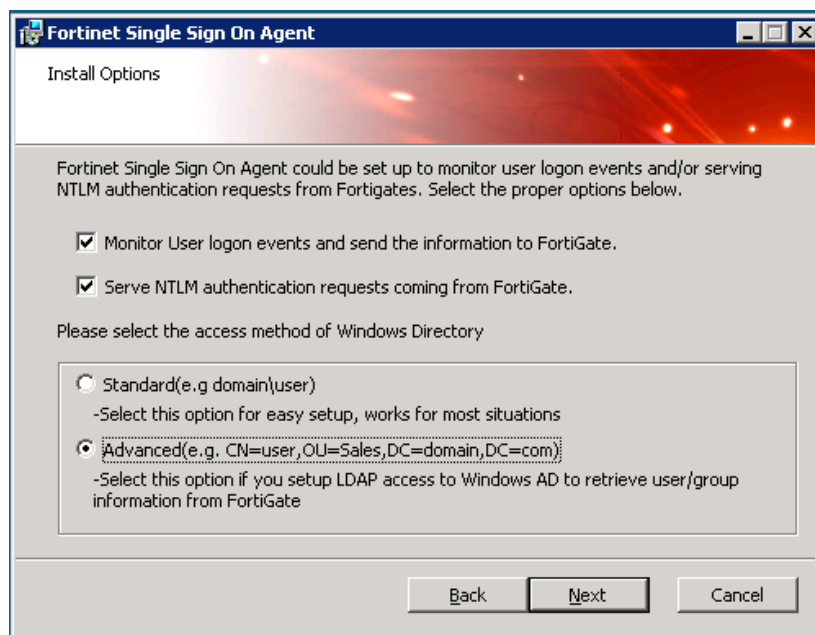
User name must be in form DomainName\UserName. If you want to use local user account, please enter .\UserName.

User Name: .\administrator

Password: \*\*\*\*\*

Back Next Cancel

### 4) Select the Advanced Mode



Install Options

Fortinet Single Sign On Agent could be set up to monitor user logon events and/or serving NTLM authentication requests from Fortigates. Select the proper options below.

☒ Monitor User logon events and send the information to FortiGate.

☒ Serve NTLM authentication requests coming from FortiGate.

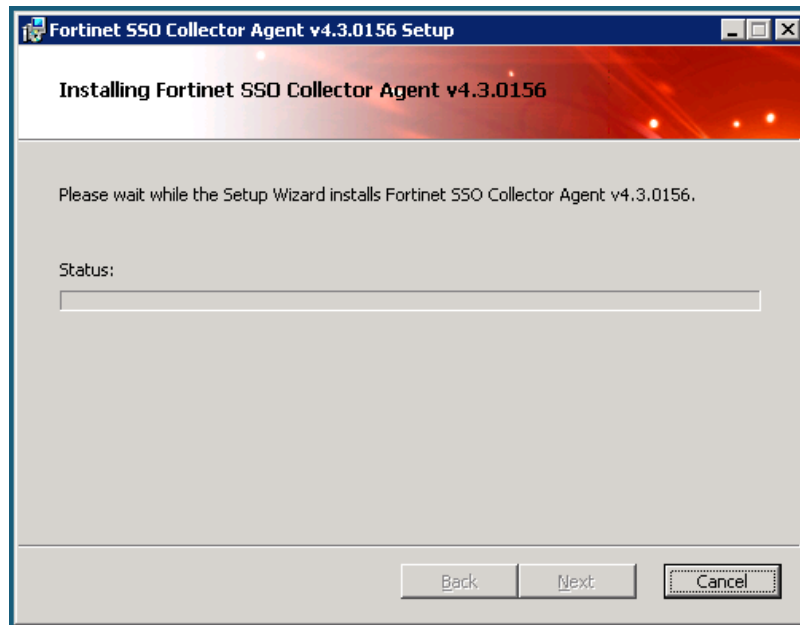
Please select the access method of Windows Directory

☐ Standard(e.g domain\user)  
-Select this option for easy setup, works for most situations

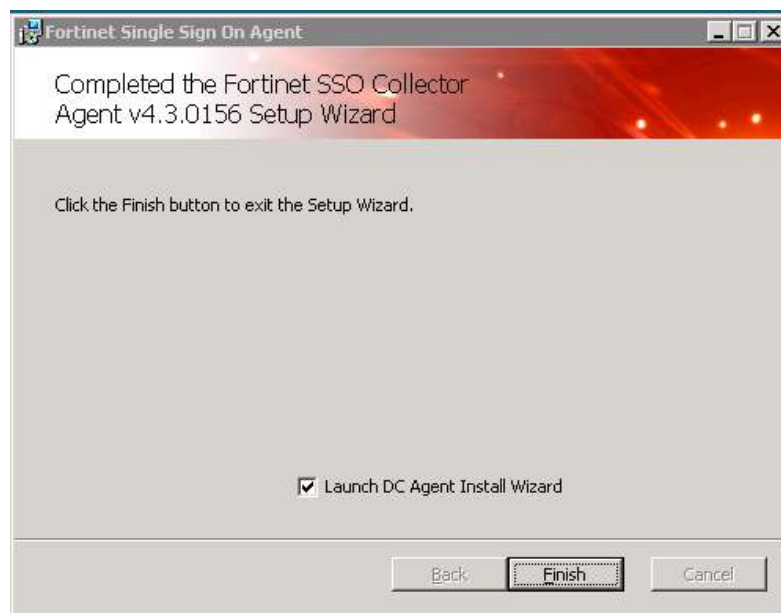
☒ Advanced(e.g. CN=user,OU=Sales,DC=domain,DC=com)  
-Select this option if you setup LDAP access to Windows AD to retrieve user/group information from FortiGate

Back Next Cancel

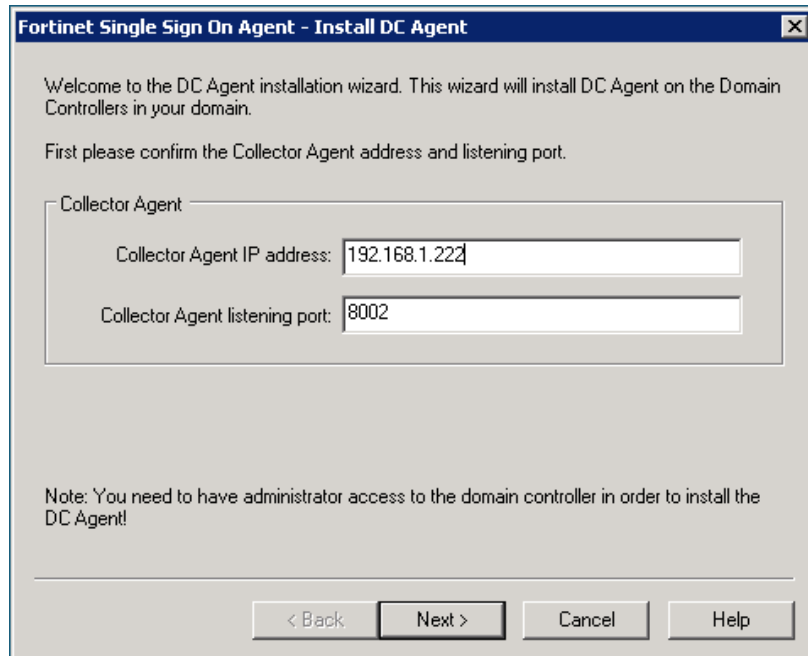
**5) Proceed to next to install the Agent**



**6) Install the DC Agent when it tries to launch**



7) You need to specify the Collector agent which the DC agent will talk to, if this is the same server, then leave the default



**Fortinet Single Sign On Agent - Install DC Agent**

Welcome to the DC Agent installation wizard. This wizard will install DC Agent on the Domain Controllers in your domain.

First please confirm the Collector Agent address and listening port.

Collector Agent

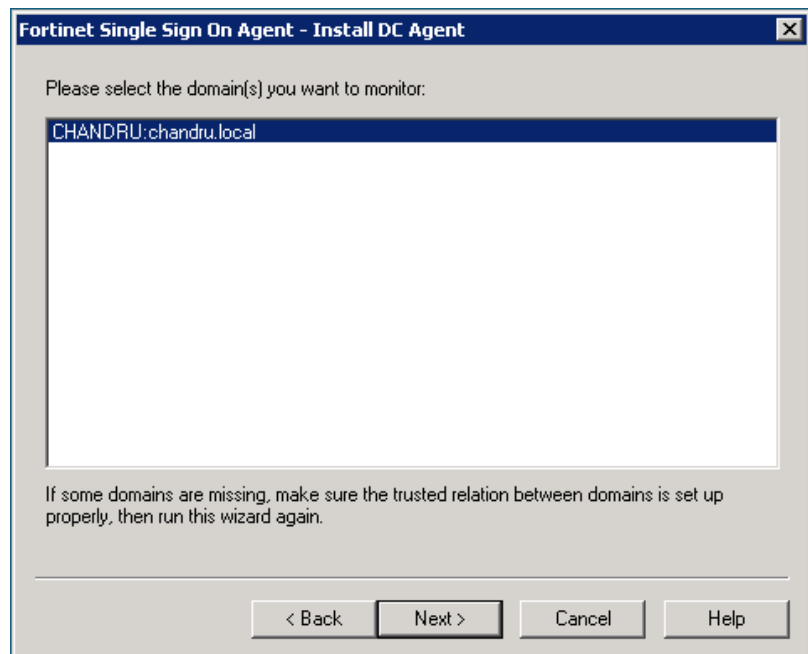
Collector Agent IP address: 192.168.1.222

Collector Agent listening port: 8002

Note: You need to have administrator access to the domain controller in order to install the DC Agent!

< Back   Next >   Cancel   Help

8) Select the Domain to monitor and click Next



**Fortinet Single Sign On Agent - Install DC Agent**

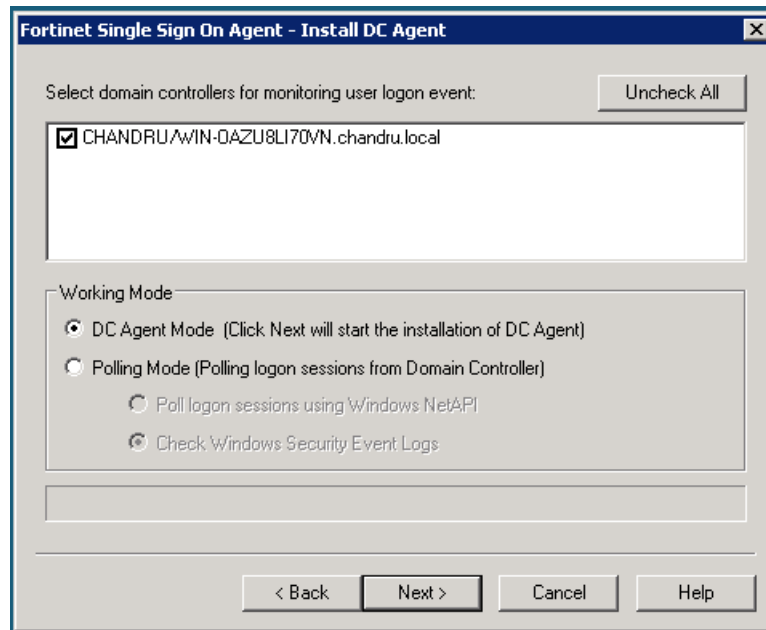
Please select the domain(s) you want to monitor:

CHANDRU:chandru.local

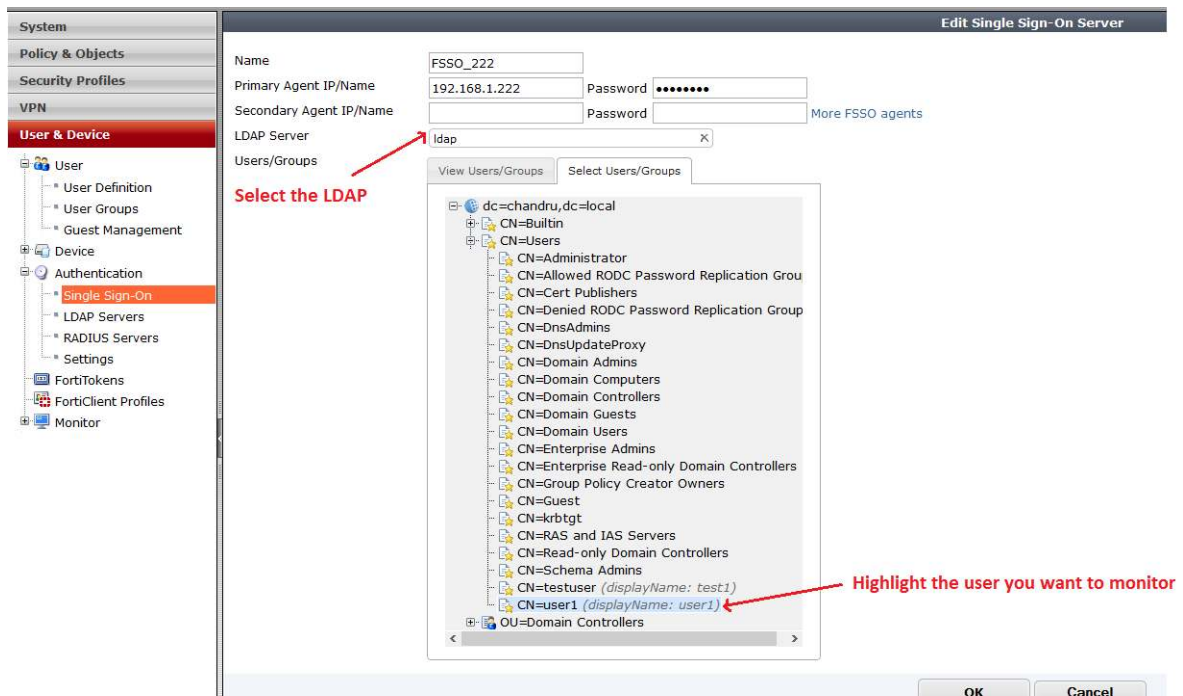
If some domains are missing, make sure the trusted relation between domains is set up properly, then run this wizard again.

< Back   Next >   Cancel   Help

9) In the Domain to monitor, select the DC Agent mode



Once the FSSO agent with DC agent is installed successfully, configure FortiGate FSSO by selecting LDAP server to filter the users



Once you select the user and click OK, you will see the user will be available

System

Policy & Objects

Security Profiles

VPN

**User & Device**

User

- User Definition
- User Groups
- Guest Management

Device

Authentication

- Single Sign-On

Edit Single Sign-On Server

Name: FSSO\_222

Primary Agent IP/Name: 192.168.1.222 Password: .....

Secondary Agent IP/Name: Password: More FSSO agents

LDAP Server: ldap

Users/Groups: View Users/Groups Select Users/Groups

user1

OK Cancel

The same user will be reflecting on the FSSO agent once it synchronizes

Fortinet Single Sign On Agent Configuration

Monitoring user

Listening ports

FortiGate: 80

Logging

Log level: W

Log logon ev

Authentication

Require auth

Timers

Workstation verify

Dead entry timeout

IP address change

Cache user g

Cache expire

FortiGate Filter List

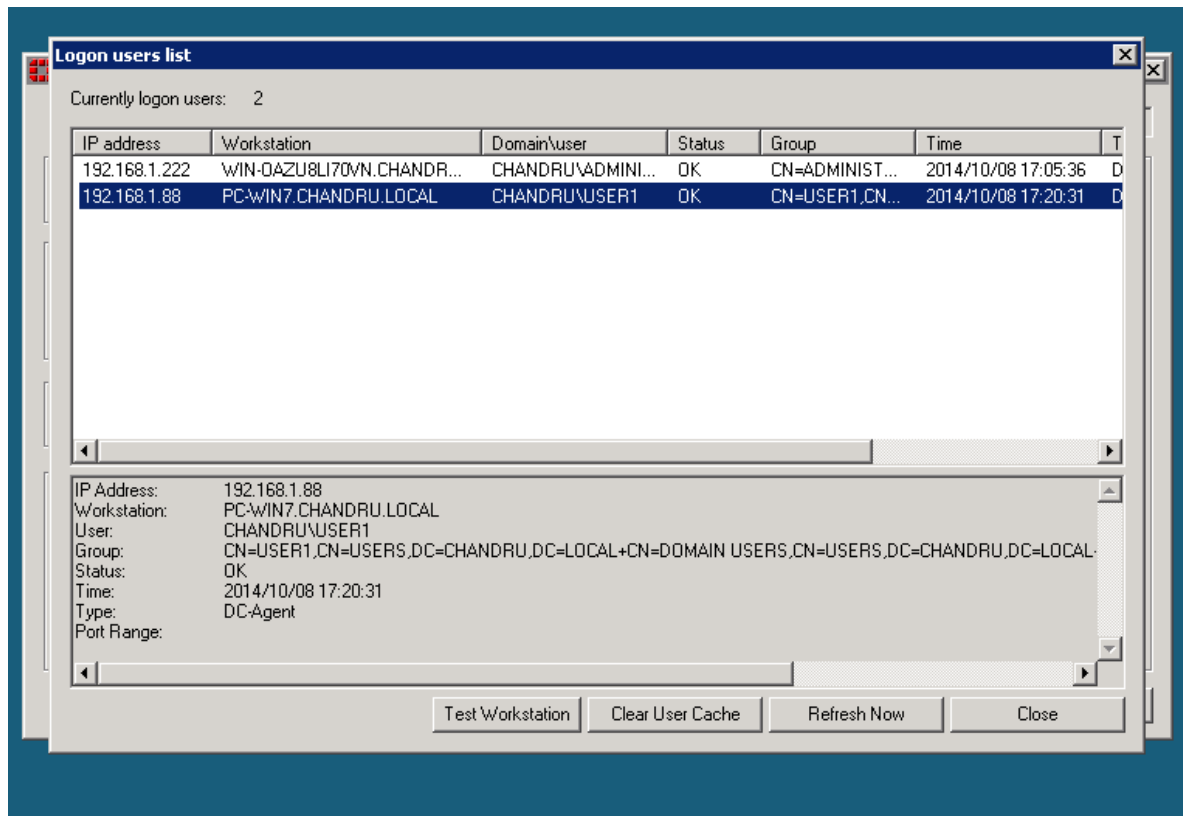
Specify monitoring groups of FortiGates. Users logon/logoff activities will only be sent to the FortiGate if the users belongs to its monitored groups. If a default filter is defined, it will be used when no matching FortiGate filter is found.

FortiGate SN	Description	Monitored groups
FGT60D4613015...	Filter set by Forti...	CN=user1,CN=Users,dc=chandru,dc=local

Add... Edit... Remove OK Cancel

Advanced Settings Save&close Apply Default Help

Domain workstation logged into the domain and created logon event on DC, the same information available on FSSO agent logon user list



On FortiGate you can see the same user:

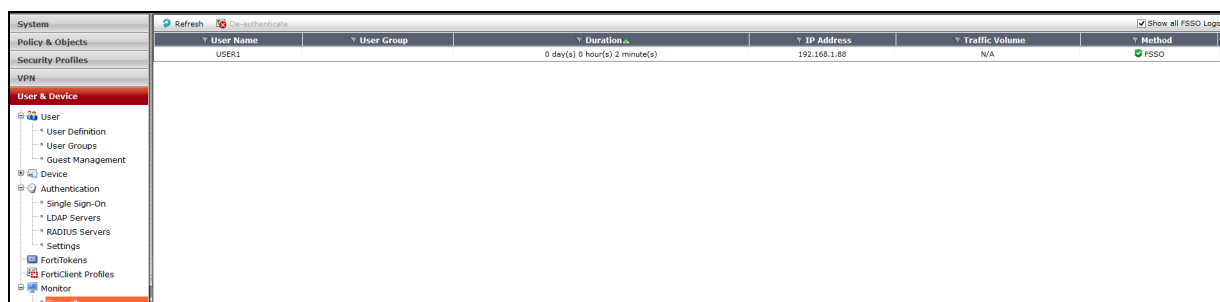
FGT60D4613015643 # diagnose debug authd fssolist

----FSSO logons----

IP: 192.168.1.88 User: USER1 Groups: CN=USER1,CN=USERS,DC=CHANDRU,DC=LOCAL Workstation: PC-WIN7.CHANDRU.LOCAL

Total number of logons listed: 1, filtered: 0

----end of FSSO logons----





## Create group on FortiGate and add the user1 to the group to authenticate to the policy

**New User Group**

Name: FSSO\_user\_test

Type: ☐ Firewall ☒ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Members: CN=user1,CN=Users,dc=chandru,dc=local X

OK Cancel

**Edit Policy**

Incoming Interface: internal

Source Address: win7

Source User(s): FSSO\_user\_test

Source Device Type: Click to add...

Outgoing Interface: wan1

Destination Address: all

Schedule: always

Service: ALL

Action: ACCEPT

**Firewall / Network Options**

☒ NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

**Security Profiles**

☐ AntiVirus: default

☒ Web Filter: default

☐ Application Control: default

☐ IPS: default

☐ Email Filter: default

☐ DLP Sensor: default

Proxy Options: default

☒ SSL Inspection: default

**Traffic Shaping**

☐ Shared Shaper: guarantee-100kbps

☐ Reverse Shaper: guarantee-100kbps

☐ Per-IP Shaper: test123

**Logging Options**

☒ Log Allowed Traffic

## Sample Web Filter logs for the user

Refresh Download Raw Log Log location: Memory

#	Date/Time	User	Source	Action	URL	Category Description	Initiator	Sent / Received
1	05:06:24	USER1	USER1 (192.168.1.88)	blocked	www.miniclip.com/favicon.ico			287 B / 0 B
2	05:06:24	USER1	USER1 (192.168.1.88)	blocked	www.miniclip.com/			607 B / 0 B